ΟΧΙ στον Προσωπικό Αριθμό και τις Ηλεκτρονικές Ταυτότητες



- Κίνδυνοι για τις ατομικές ελευθερίες και την ιδιωτικότητα
- Κίνδυνοι για την προσωπική και εθνική ασφάλεια
- Η θέση και η πρόσκληση της ΝΙΚΗΣ



www.NIKH.gr

Από το χάρτινο φακέλωμα της δικτατορίας... στο ηλεκτρονικό φακέλωμα της «δημοκρατίας».

• 1981: Καταργήθηκε το παραδοσιακό «φακέλωμα»

Το «πιστοποιητικό πολιτικών φρονημάτων» καταργήθηκε επισήμως το 1981. Το 1989 περισσότερα από 17 εκατομμύρια έγγραφα «φακελώματος» πολιτών ρίφθηκαν τελικώς στην πυρά.

• 2001: Αφαιρέθηκε το θρήσκευμα και το δακτυλικό αποτύπωμα από τις ταυτότητες.

Στο παρελθόν έγινε τόση φασαρία να αφαιρεθεί το θρήσκευμα από τις ταυτότητες επειδή θεωρήθηκε ευαίσθητο προσωπικό δεδομένο.
Επίσης καταργήθηκε το δακτυλικό αποτύπωμα διότι παρέπεμπε σε υποψίες εγκλήματος. Από τη «σήμανση» των δακτυλικών αποτυπωμάτων προέρχεται και η έκφραση «σεσημασμένος».

• 2024: Επιβάλλονται, χωρίς αντικειμενικό σκοπό, νέες ηλεκτρονικές ταυτότητες με chip.

Η ΕΕ υποχρεώνει στην έκδοση ηλεκτρονικών ταυτοτήτων με μικροκύκλωμα (chip) ΜΟΝΟ όταν αυτές χρησιμοποιούνται ως ταξιδιωτικά έγγραφα. Για εθνική χρήση, και για τις συναλλαγές του πολίτη με το κράτος, έχουμε πλήρη ελευθερία να διατηρούμε εναλλακτικά μέσα ταυτοποίησης (δελτίο ταυτότητας, δίπλωμα οδήγησης, διαβατήριο κ.α.).

Η απαιτούμενη ασφάλεια για τα μέσα ταυτοποίησης επιτυγχάνεται εύκολα και οικονομικά με νέες εκτυπωτικές τεχνολογίες, που δεν παραχαράσσονται εύκολα, όπως, για παράδειγμα, τα διπλώματα οδήγησης.

ΚΑΝΕΙΣ δεν υποχρέωσε την ελληνική κυβέρνηση να επιβάλει ηλεκτρονικές ταυτότητες με **RFID chip** σε εθνικό επίπεδο, δηλαδή ταυτότητες που μπορούν να ιχνηλατούνται και να προσφέρουν σε τρίτους πληροφορίες ερήμην του κατόχου τους.

• Σήμερα αποκαλύπτεται ο δόλιος σκοπός της κυβέρνησης ΝΔ για τις νέες ηλεκτρονικές ταυτότητες: η υποχρεωτική ενσωμάτωση του Προσωπικού Αριθμού.

• Ο Προσωπικός Αριθμός συγκεντρώνει όλα τα προσωπικά μας δεδομένα, και τα παραδίδει στις ορέξεις οποιασδήποτε μελλοντικής κυβέρνησης της Ελλάδας ή διευθυντηρίου της ΕΕ.

• **Σεπτέμβριος 2020*:** Η κυβέρνηση της ΝΔ θεσπίζει Προσωπικό Αριθμό για την «υποχρεωτική επαλήθευση της ταυτότητας των φυσικών προσώπων στις συναλλαγές τους με τους φορείς του δημόσιου τομέα». Ο Π.Α. αποτελείται από «δώδεκα (12) αλφαριθμητικά στοιχεία, εκ των οποίων τουλάχιστον τα εννέα (9) είναι αριθμητικά» (που τελικά είναι ο ΑΦΜ). Ο Π.Α. δεν μεταβάλλεται και τα δεδομένα του τηρούνται απεριόριστα και μετά τον θάνατο του φυσικού προσώπου.

• **Μάρτιος 2025**: Η κυβέρνηση της ΝΔ συνδέει τον** Προσωπικό Αριθμό με τις νέες ηλεκτρονικές ταυτότητες, οι οποίες πλέον και τον αποθηκεύουν στο chip αλλά και τον αναγράφουν εμφανώς, με πρόσχημα την διευκόλυνση των συναλλαγών. Η νομοθεσία «περνά» δόλια και ύπουλα ως μεταμεσονύχτια τροπολογία, και χωρίς πλήρη έγκριση της Ανεξάρτητης Αρχής Προστασίας Προσωπικών Δεδομένων για τον τρόπο που υλοποιείται ο Προσωπικός Αριθμός, ενώ υπουργοί της ΝΔ μεταδίδουν ασύστολα ψέματα στα ΜΜΕ για την υποχρεωτικότητα, την ασφάλεια και τον σκοπό του μέτρου.

• **Μάιος 2025***:** Με αντισυνταγματικό Προεδρικό Διάταγμα, η κυβέρνηση θέτει σε εφαρμογή τον Προσωπικό Αριθμό στις νέες ηλεκτρονικές ταυτότητες.

• Ο ιατρικός μας φάκελος, η ασφαλιστική ενημερότητα, τα οικονομικά μας, τα βιομετρικά μας δεδομένα, τα γεωγραφικά ίχνη των συναλλαγών μας, μπορούν και ενοποιούνται μέσω του Προσωπικού Αριθμού, τον οποίον ενσωματώνει η νέα ηλεκτρονική ταυτότητα, μάλιστα χωρίς καν τη συγκατάθεσή μας. Πρόκειται για τον ορισμό του φακελώματος!

Η δήθεν «διευκόλυνση των συναλλαγών» είναι η μεγαλύτερη ψευδοδικαιολογία για να επιβληθεί φακέλωμα χειρότερο από εκείνο οποιασδήποτε δικτατορίας. Πριν 36 χρόνια κάψαμε τους «φακέλους φρονημάτων», σήμερα λέμε ζήτω οι ηλεκτρονικοί φάκελοι!

** Ν.4727/2020 ** Ν. 5188/2025 άρθ.31 *** Προεδρικό Διάταγμα 40/2025*

Από την αθώα ταυτοποίηση στο επικίνδυνο profiling

Ταυτοποίηση σημαίνει...
...απλή επιβεβαίωση για το ποιος είμαι.

Είστε αυτός που λέει το εισιτήριο!



“Profiling”, ή “Φακέλωμα”, ή κάποτε “Αυτοματοποιημένη επεξεργασία δεδομένων”, σημαίνει... πρόσβαση σε δικαιώματα, που σήμερα έχεις και αύριο ίσως όχι.

Είναι αυτός που λέει το εισιτήριο...



Ναι αλλά επίσης...

- Είναι διαβητικός
- Δεν έχει φορολογική ενημερότητα
- Δεν έκανε την 3η δόση εμβολίου
- Χρωστά 2 πρόστιμα παράνομης στάθμευσης
- Δεν ψήφισε στις εκλογές

ΑΡΑ
σύμφωνα με το σύστημα αξιολόγησης δεν δικαιούται να ταξιδέψει σήμερα...

Ο Γενικός Κανονισμός Προσωπικών Δεδομένων (GDPR) επιτάσσει την «αρχή της αναλογικότητας», δηλαδή το κράτος να τηρεί μόνο τα ελάχιστα, απολύτως απαραίτητα δεδομένα, έτσι ώστε ο πολίτης να προστατεύεται από κάθε είδους κατάχρηση των δεδομένων του.

Η σωστή εφαρμογή της «αρχής της αναλογικότητας» σε ένα κράτος που σέβεται την ιδιωτικότητα του πολίτη: **Αν κάποιος αριθμός παραβιαστεί (π.χ. διαρροή ΑΦΜ), η ζημιά περιορίζεται στον συγκεκριμένο τομέα.**



Αντίθετα, ο Προσωπικός Αριθμός παραβιάζει την ιδιωτικότητα, επιτρέπει αδιάκριτη αναγνώριση παντού και ενέχει κίνδυνο ανεξέλεγκτης διαρροής δεδομένων. Είναι ένα καθολικό PIN (Personal Identification Number) στη ζωή μας που μάλιστα, σε αντίθεση με τους συνηθισμένους κανόνες ασφαλείας, δεν το αλλάζουμε ποτέ!

Η παραβίαση της «αρχής της αναλογικότητας» σε κράτος που εφαρμόζει Προσωπικό Αριθμό: **Με έναν καθολικό Προσωπικό Αριθμό, μια παραβίαση εκθέτει το σύνολο των προσωπικών μας στοιχείων.**



Η διάτρητη ασφάλεια των προσωπικών δεδομένων μας στην Ελλάδα...

Σημαντικές κυβερνοεπιθέσεις έχουν σημειωθεί στην Ελλάδα, θέτοντας σε αμφισβήτηση την ασφάλεια των ψηφιακών συστημάτων που αποθηκεύουν προσωπικά δεδομένα:

• Το Ελληνικό Ανοικτό Πανεπιστήμιο, όπου το 2024 σημειώθηκε εκτεταμένη κλοπή προσωπικών δεδομένων: ένας τεράστιος όγκος 813 GB πληροφοριών με προσωπικά δεδομένα φοιτητών του ΕΑΠ διέρρευσε στο dark web .

• Οι υπηρεσίες των Gov.gr και TAXIS-net, όπου άγνωστοι κυβερνοεγκληματίες από την Ολλανδία με πρωτοφανή επίθεση επιχείρησαν να θέσουν εκτός λειτουργίας 800 κυβερνητικές ιστοσελίδες, «παγώνοντας» ηλεκτρονικές ιατρικές συνταγές.

• Το Υπουργείο Παιδείας, με στόχο μια κεντρική πλατφόρμα εξετάσεων λυκείου, προκαλώντας διακοπές λειτουργίας και καθυστερήσεις.

• Το Υπουργείο Προστασίας του Πολίτη, την ιστοσελίδα αξιολόγησης του ΙΕΠ, το Υπουργείο Εξωτερικών (θύμα των Anonymous), το Εθνικό Τυπογραφείο, τη Βουλή των Ελλήνων (θύμα των «Real Democracy Reverse Engineering»).

Σημαντικά πρόστιμα στο ίδιο το κράτος και σε ιδιωτικές εταιρείες έχει επιβάλει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για σημαντικές παραβιάσεις του GDPR. Ενδεικτικά:

• **Πρόστιμο 150.000€ στο Υπουργείο Προστασίας του Πολίτη** για παραβιάσεις στις νέες ταυτότητες (2024) – συγκεκριμένα, 50.000€ για παραβιάσεις υποχρεώσεων πληροφόρησης και 100.000€ για μη διενέργεια Εκτίμησης Επιπτώσεων στην Προστασία Δεδομένων (DPIA).

• **Πρόστιμο 400.000€ στο Υπουργείο Εσωτερικών και 40.000€ σε υποψήφια ευρωβουλευτή της Νέας Δημοκρατίας** (2024) για παράνομη διαρροή και προεκλογική χρήση emails Αποδήμων ψηφοφόρων. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε τα παραπάνω πρόστιμα, με τη διαρροή να αφορά ξεκάθαρα σε εσωτερική παραβίαση και όχι εξωτερικό παράγοντα ή τεχνική παραβίαση μέτρων ασφαλείας. Με απλά λόγια, ο καθησυχασμός και οι διαβεβαιώσεις περί ασφάλειας των συστημάτων, δεν σημαίνει τίποτα όταν μία διεφθαρμένη κυβέρνηση αποκτήσει πρόσβαση στα προσωπικά δεδομένα μας.

• **Υπόθεση Clearview AI και πρόστιμο 20 εκατ. ευρώ** (2022): Η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε το μεγαλύτερο ιστορικά πρόστιμο στην αμερικανική εταιρεία Clearview AI για παράνομη χρήση τεχνολογίας αναγνώρισης προσώπου και συλλογή βιομετρικών δεδομένων για Έλληνες πολίτες, χωρίς την συγκατάθεσή τους. Συνολικά πρόστιμα άνω των 100 εκ € επεβλήθησαν και από άλλα ευρωπαϊκά κράτη (Γαλλία, Ιταλία, Ολλανδία, Αυστρία), με την απαίτηση η εταιρεία να διαγράψει τα δεδομένα των Ευρωπαίων πολιτών, σύμφωνα με την Ευρωπαϊκή Επιτροπή Προστασίας Δεδομένων.

• **Σκάνδαλο παρακολουθήσεων πολιτικών και δημοσιογράφων από την ΕΥΠ με το λογισμικό Predator** (2022): Το 2022 αποκαλύφθηκε ότι η Εθνική Υπηρεσία Πληροφοριών παρακολουθούσε παράνομα πολιτικούς, δημοσιογράφους και άλλους δημόσιους λειτουργούς. Η υπόθεση που έγινε γνωστή και ως "Ελληνικό Γουώτεργκέιτ", αναδεικνύει πόσο ευάλωτη είναι η ιδιωτικότητα της ζωής κάθε πολίτη, όταν στο κράτος προσφερθούν οι τεχνολογικές ευκαιρίες, που του επιτρέπουν την αδιαφανή χρήση ψηφιακών τεχνολογιών για αλλότριους σκοπούς.

...αλλά και σε οργανωμένα μεγάλα κράτη.

Πολλές κυβερνήσεις ανά τον κόσμο καταχρώνται τις ψηφιακές τεχνολογίες για να παρακολουθούν ή να ελέγχουν τους πολίτες τους. Η ανησυχία για τα προσωπικά μας δεδομένα, τις μελλοντικές προσωπικές ελευθερίες και τα δικαιώματα των παιδιών μας είναι μεγαλύτερη από ποτέ. Θυμίζουμε ενδεικτικά:

• **ΗΠΑ - Παρακολούθηση Πολιτών (NSA και Snowden):** Η πιο διάσημη περίπτωση παράνομης παρακολούθησης τηλεφωνικών κλήσεων και διαδικτυακής δραστηριότητας εκατομμυρίων πολιτών, τόσο εντός των ΗΠΑ όσο και διεθνώς, είναι το σκάνδαλο της Εθνικής Υπηρεσίας Ασφαλείας (NSA) των ΗΠΑ, που αποκάλυψε ο Edward Snowden το 2013.

• **Καναδάς - Παρακολούθηση Διαδηλωτών (2022):** Η μαζικότατη διαμαρτυρία του “Freedom Convoy” για τα παράλογα μέτρα εγκλεισμού επί Covid-19, αντιμετωπίστηκε από την κυβέρνηση με τεχνολογίες αναγνώρισης βιομετρικών δεδομένων των διαδηλωτών πολιτών, και με το πάγωμα των τραπεζικών τους λογαριασμών. Αύριο στην Ελλάδα, ο Προσωπικός Αριθμός και η σύνδεση των βάσεων δεδομένων θα επιτρέπει ακριβώς και στις εδώ κυβερνήσεις ανάλογες πρακτικές επιβολής.

• **Ινδία – Ψηφιακή Ταυτότητα “Aadhaar”:** Αυτό που αρχικά διαφημίστηκε ως εύκολη πρόσβαση των πολιτών σε κυβερνητικές υπηρεσίες, γρήγορα έγινε εργαλείο συλλογής δεδομένων και παρακολούθησης, ενώ το 2018 η κρατική βάση δεδομένων των ταυτοτήτων υπέστη πολλαπλές διαρροές, εκθέτοντας προσωπικά δεδομένα δυνητικά 1.1 δισεκατομμυρίων πολιτών.



• **Κίνα - Ψηφιακή Επιτήρηση (Social Credit System):** Η κυβέρνηση παρακολουθεί τους πολίτες και τους βαθμολογεί, με αντίκτυπο στην διατήρηση ή στέρηση δικαιωμάτων, στη χρηματοδότηση, στις μετακινήσεις κλπ. Ο Κλάους Σβαμπ του Παγκόσμιου Οικονομικού Φόρουμ επαίνεσε το σύστημα αυτό καθώς «θα μπορούσε να αποτελέσει πρότυπο για πολλά έθνη».

Αντίστοιχα, κυβερνοεπιθέσεις δεν έχουν αφήσει άτρωτους κολοσσούς του διεθνούς στερεώματος.

• Πάνω από 30 εκατομμύρια προσωπικά αρχεία παραβιάστηκαν σε πέντε μεγάλες κυβερνοεπιθέσεις το 2023, σε υπουργεία της Νορβηγίας, το αμερικανικό δίκτυο φαρμακείων PharMerica, την εφαρμογή “MOVEit” της Genworth Financial, την MCNA Dental και τη Latitude Financial.

• Πέντε από τις χαρακτηριστικότερες μεγάλης κλίμακας κυβερνοεπιθέσεις έπληξαν την Yahoo! (2014, 500 εκατ. λογαριασμοί), τη River City Media (2017, 1.4 δισεκατ. αρχεία), την εφαρμογή MyFitnessPal της UnderArmour (2018, 144 εκατ. επαφές), το Πεντάγωνο των ΗΠΑ, μέχρι και πυρηνικό σταθμό σύμφωνα με τον πρόεδρο του Διεθνούς Οργανισμού Ατομικής Ενέργειας.

Γιατί είναι επικίνδυνη η ενοποίηση των προσωπικών μας δεδομένων;

• Γιατί επιτρέπει σε μία τωρινή ή μελλοντική κυβέρνηση να επιβάλει εκδικητικά μέτρα σε αντιφρονούντες

• Άλλο η πρόσβαση ενός υπαλλήλου σε μία υπηρεσία και άλλο η πρόσβαση της κεντρικής κυβέρνησης σε ενοποιημένο προφίλ πολιτών. Χωρίς επαρκείς μηχανισμούς διαφάνειας, μπορεί ο ΠΑ να χρησιμοποιηθεί για αυθαίρετες διασταυρώσεις, αποκλεισμούς πολιτών για λόγους δήθεν «εθνικής ασφάλειας» ή ακόμα και για πολιτικούς σκοπούς, διαμορφώνοντας εκλογικό αποτέλεσμα, όπως π.χ. με την αφαίρεση του δικαιώματος ψήφου στους ανεμβολίαστους μιας αυριανής «πανδημίας».

• Μπορεί να τιμωρηθεί αθόρυβα η ελευθερία του λόγου και η νόμιμη έκφραση διαφωνίας, εφαρμόζοντας πιέσεις σε θεμελιώδη δικαιώματα, που σήμερα μας φαίνεται αδιανόητο να προσβληθούν.

• Ας φανταστούμε ότι σήμερα χρωστούμε στο Δημόσιο ή κάνουμε μια δήλωση που δεν συμφωνεί με τις “προδιαγραφές”. Αύριο, είναι πιθανό να μη μπορείς να βγάλεις εισιτήριο, να πληρωθείς, να αγοράσεις φάρμακο ή να μπεις στο ΚΤΕΛ. Όχι γιατί δεν έχεις χρήματα ή δικαιώματα, αλλά γιατί ο Προσωπικός σου Αριθμός έχει «φραγεί» από το σύστημα. Δεν είναι θεωρία. Είναι τεχνικά εφικτό και ήδη εφαρμόζεται αλλού, όπως εξηγήσαμε.

• Γιατί γίνεται εύκολο να επιβληθούν δυσμενείς συνέπειες στον πολίτη και στον ιδιωτικό τομέα

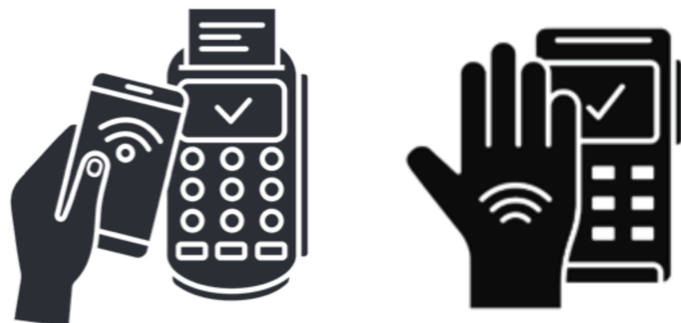
• Το προφίλ κοινωνικής και διαδικτυακής συμπεριφοράς μας θα μπορεί να συνιστά κριτήριο πρόσληψης, να προσδιορίζει δικαιώματα πρόσβασης στους τραπεζικούς λογαριασμούς μας, σε εργασιακές παροχές, ή στα δικαιώματα σύνταξης.
• Το προφίλ κατάστασης υγείας θα μπορεί να προσδιορίζει κριτήρια ή κόστος υποχρεωτικής ασφάλισης και ιατροφαρμακευτικής κάλυψης, ακόμη και κριτήριο πρόσληψης, καταπατώντας κάθε έννοια ίσης πρόσβασης στην εργασία.

• Γιατί οι συνέπειες κλοπής είναι και πιθανές και δραματικές

• Η χρήση ενός μοναδικού αριθμού για όλες τις συναλλαγές με το Δημόσιο (και μελλοντικά και με ιδιωτικούς φορείς) καθιστά πιο εύκολη τη δημιουργία πλήρους προφίλ για κάθε πολίτη. Η παραβίαση μίας βάσης δεδομένων, αποκαλύπτει το πλήρες ψηφιακό αποτύπωμα ενός προσώπου. Κλέβουν την ζωή μας ολόκληρη. Όπως είναι φρόνιμο να μην ανοίγουμε το σπίτι μας σε απρόσκλητους άγνωστους, το ίδιο φρόνιμο είναι να προστατεύουμε και το «ψηφιακό» σπίτι μας.
• Ακόμη περισσότερο, μια **διαρροή προσωπικών δεδομένων των Ενόπλων Δυνάμεων και των Σωμάτων Ασφαλείας θέτει σε προφανείς κινδύνους την εθνική μας ασφάλεια και κυριαρχία.**

Ποια είναι η μεγάλη εικόνα;

Ο Προσωπικός Αριθμός, η αντικατάσταση του μετρητού χρήματος σε ηλεκτρονικό χρήμα, το Ψηφιακό Ευρώ, μπορεί να φαίνονται εκ πρώτης όψεως ως μέτρα διευκόλυνσης της ζωής μας.
Όμως, στο κοντινό «αύριο», συνδυαστικά δομούν ένα ενιαίο, υποχρεωτικό σύστημα που συγκεντρώνει ταυτοποίηση, πληρωμές, ιατρικά δεδομένα, βιομετρική αναγνώριση προσώπου, πρόσβαση σε υπηρεσίες. Κάθε οικονομική μας πράξη γίνεται γνωστή σε τρίτους στο διηνεκές – και μάλιστα, γνωστή σε υπαλλήλους μιας σημερινής ή αυριανής κυβέρνησης με απεριόριστη πρόσβαση και με άγνωστες προθέσεις.



Στο επίσης κοντινό «μεθαύριο», κάποιοι ίσως πιστέψουν ότι είναι ελάχιστη η διαφορά μεταξύ ενός microchip ανέπαφης συνδεσιμότητας, ενσωματωμένου στην πλαστική κάρτα-ταυτότητα, με ένα αντίστοιχο microchip εμφυτευμένο στο σώμα μας, για να μην υπάρχουν απώλειες.



Και τότε, για χάρη της άνεσης και της ασφάλειας, θα γίνουμε σκλάβοι χωρίς επιστροφή.

Δεν χρειάζεται Προσωπικός Αριθμός για να «νοικοκυρέψουμε» το δημόσιο και ο πολίτης να έχει καλύτερες δημόσιες υπηρεσίες.

Άλλο η αληθινή βελτίωση των υπηρεσιών, και άλλο η προσθήκη ενός ακόμη ψηφιακού αριθμού στη γραφειοκρατεία.

• **Δεν χρειάζεται ενιαίος Προσωπικός Αριθμός για να επιτευχθεί διαλειτουργικότητα στο Δημόσιο.**
Οι υπηρεσίες μπορούν ήδη να επικοινωνούν με βάση τον ΑΔΤ, ΑΦΜ, τον ΑΜΚΑ ή άλλους αριθμούς. Η αντιστοίχιση ΑΔΤ, ΑΦΜ και ΑΜΚΑ έχει ήδη επιτευχθεί στο Εθνικό μητρώο που διαχειρίζεται η Ηλεκτρονική Διακυβέρνηση Κοινωνικής Ασφάλισης (Η.ΔΙ.Κ.Α.) Η επαλήθευση του πολίτη στις συναλλαγές του με το Δημόσιο, εξ ορισμού εξυπηρετείται από τον Αριθμό Δελτίου Ταυτότητας (ΑΔΤ) χωρίς ανάγκη ενός νέου μητρώου Προσωπικού Αριθμού.

• **Δεν χρειάζεται ενιαίος Προσωπικός Αριθμός για την επικαιροποίηση των προσωπικών στοιχείων των Ελλήνων πολιτών.** Η επικαιροποίηση πραγματοποιείται χωρίς την ανάγκη του Προσωπικού Αριθμού και μάλιστα, όπως ομολογεί η κυβέρνηση, πρέπει να προηγηθεί πριν από την έκδοση του Προσωπικού Αριθμού.

Το κράτος νοικοκυρεύεται όταν η κυβέρνηση σκύψει στα καθημερινά προβλήματα του απλού Έλληνα.

• **Δεν χρειάζεται ενιαίος Προσωπικός Αριθμός για να διευκολύνονται οι συναλλαγές μας με το Δημόσιο.**
Η ευκολία δεν προκύπτει από τον ΠΑ, αλλά από το αν οι υπηρεσίες είναι καλά οργανωμένες.

> Ας θυμηθούμε την καθυστέρηση ακόμη και για παραπάνω από έτος της έκδοσης σύνταξης σε όποιον συνταξιοδοτείται!

> Ας θυμηθούμε την άρνηση συμψηφισμού των οφειλών του κράτους απέναντι στον πολίτη!

> Ας θυμηθούμε την ανεπαρκή αρχειοθέτηση με τα ανύπαρκτα αρχεία παλαιών διπλωμάτων οδήγησης!

> Ας θυμηθούμε την ανάγκη ενημέρωσης των ληξιαρχείων, ώστε να αποφεύγεται η άπειρη ταλαιπωρία των συγγενών κάθε θανόντος συμπολίτη μας για να τακτοποιήσουν κάθε εκκρεμότητα!

Αυτά θα νοικοκυρέψουν το κράτος, και όχι ο ψηφιακός έλεγχος της κυβέρνησης πάνω στη ζωή των πολιτών!

Η ελαφρότητα των τοποθετήσεων κυβερνητικών στελεχών προκαλεί βάσιμους φόβους για τις προθέσεις τους.

• ***«Ήδη δίνετε τα προσωπικά σας δεδομένα στην Google, στο Facebook, στις εταιρίες κινητής τηλεφωνίας – γιατί σας πειράζουν τα δεδομένα του Προσωπικού Αριθμού;»***

• Συχνά μπορεί να δίνουμε προσωπικά μας δεδομένα για να χρησιμοποιήσουμε απαραίτητες λειτουργίες στο κινητό μας τηλέφωνο, υπηρεσίες πλοήγησης σε χάρτες, ή σε μέσα κοινωνικής δικτύωσης. Το κάνουμε εθελοντικά, προαιρετικά, με ρητή μας συναίνεση που την ανακαλούμε όποτε θέλουμε, και με αντάλλαγμα υπηρεσίες που επιλέγουμε, όταν τις επιθυμούμε.

• ***«Έχετε ΑΦΜ, ΑΜΚΑ, Δελτίο Ταυτότητας, και μπερδεύεστε. Τι σας πειράζει ένας ακόμη κωδικός, που μάλιστα δεν θα χρειάζεται να θυμάστε κανέναν άλλον;»***

• Χωρίς να καταργεί τον ΑΦΜ και τον ΑΜΚΑ, ο Προσωπικός Αριθμός ενοποιεί όλες τις βάσεις δεδομένων σε μία λογική βάση, στην οποία δεν ελέγχεις ποιοι φορείς τον χρησιμοποιούν, πότε, ή για ποιον λόγο. Ο Προσωπικός Αριθμός δημιουργεί συσχετισμούς χωρίς να γνωρίζεις και χωρίς να συναινείς σε αυτούς.

• ***«Μα έχετε τίποτα να κρύψετε, και γι'αυτό δεν θέλετε τον Προσωπικό Αριθμό;»***

• Το δικαίωμα κάθε πολίτη στην ιδιωτικότητα δεν έχει σχέση με το αν έχεις να «κρύψεις» κάτι. Είναι δικαίωμα να μην παρακολουθείσαι, να μη συγκεντρώνονται δεδομένα σου χωρίς όριο, και να μη γίνεται μαζική επεξεργασία χωρίς έλεγχο.

• ***«Γιατί αντιδράτε σε κάτι που είναι εξάλλου καθολικό για όλους;»***

• Σήμερα τίθενται τα σκοτεινά θεμέλια για ένα σύστημα που δεν έχει όρια στην παρακολούθηση της ιδιωτικής ζωής των πολιτών. Αν δεν αντιδράσουμε, σημαίνει ότι αφήνουμε στα παιδιά μας μια κληρονομιά ψηφιακής υποδούλωσης στην οποία οι επιλογές και οι ελευθερίες τους βρίσκονται σε άμεσο κίνδυνο. Η ιδιωτικότητα είναι θεμελιώδες δικαίωμα, όχι πολυτέλεια.

• Η σημερινή μας αντίσταση θεμελιώνει την μελλοντική ελευθερία των παιδιών μας.